UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,108	11/16/2001	Michael Burrows	18973-49 (P00-3010)	2868

7590 08/04/2005

Attn: Richard P. Lange
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/991,108	BURROWS ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40 and 42-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 58 have been presented for examination. Claim 41 has been cancelled and claims 1, 8, 22, 24, 25, 40, 44 have been amended; and new claims 59 – 63 have been added in an amendment filed 6/9/2005.

Response to Arguments

2. Applicant's arguments filed on 06/09/2000 with respect to most of instant claims have been fully considered but are moot in view of the new ground(s) of rejection.

3. As per claim 42, Applicant remarks "Bass does not disclose the means for monitoring the network for any patterns of behavior, including, if available, information about a pattern of behavior from any of the computers about another one of the computers (Page 17, 2nd Para Line 4 – 6). Examiner notes Applicant's arguments have been fully considered but are not persuasive because (a) the number of multiple destination messages received is interpreted as "information about a pattern of behavior" (Bass: Column 2 Line 48), (b) the network device is interpreted as being used for "monitoring the network" (Bass: Column 2 Line 45 – 58), and (c) the information of monitored multiple destination messages from the said network device about another computers that broadcasts the message to multiple destination computers (Bass: Column 2 Line 45 – 58) is interpreted as "information about a pattern of behavior from any of the computers about another one of the computers" to meet the claim language, where Examiner notes the network device receives the multiple destination messages

and categorize the information into one of the broadcast message class and then further validate whether the broadcast message class count exceeds a predefined threshold (Bass: Column 2 Line 45 – 58). Furthermore, Applicant argues "Leeds dos not disclose determining if the information about the pattern of behavior from any of the computers is trustworthy" (Page 18, 2nd Para Line 1 – 3). Examiner notes Leeds teaches the receiver would know immediately that the sender is not trustworthy (Leeds: Column 7 Line 12 – 13) and consequently, the information about the pattern of behavior (i.e. email spam) conveyed by the sender is thereby not trustworthy to meet the claim language.

Furthermore, Applicant remarks the combination of Bass with Leeds is using impermissible hindsight that involves piecing together completely un-related elements of prior art references to achieve the claimed invention. Examiner notes Applicant's arguments have been fully considered but are not persuasive. The reasons have two folds:

- It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Leeds within the system of Bass because (I) Bass teaches providing an improved scheme in the prevention or suppression of broadcast traffic storm in computer networks (Bass: Column 2 Line 6 – 8) and (II) Leeds teaches providing an effective and security enhanced mechanism to prevent broadcast traffic storm in the networks by using a email filter associated with an authenticator (Leeds: see for example, Column 1 Line 10 – 16, Column 2 Line 26 – 51).

- In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 5, 6, 8, 12 – 14, 16, 18, 19, 22, 26, 27, 29, 32, 33, 35, 37 – 38, 42, 45 – 50, 52 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465).

As per claim 1 and 22, Bass teaches a method for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

monitoring the network for any patterns of behavior (Bass: see for example, Column 3 Line 37 – 38);

determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior (Bass: see for example, Column 3 Line 58 – 62);

determining a proper action for mitigating that type of undesirable behavior, the proper action including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable (Bass: see for example, Column 3 Line 35 – 57).

Bass does not teach wherein preventing dissemination comprises at least one of changing a routing table, changing a forwarding table, filtering on Internet Protocol (IP) addresses, and filtering on media access control (MAC) addresses.

Leeds teaches wherein preventing dissemination comprises changing a routing table (Leeds, Column 6 Line 59 – 62).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Leeds within the system of Bass because (I) Bass teaches providing an improved scheme in the prevention or suppression of broadcast traffic storm in computer networks (Bass: Column 2 Line 6 – 8) and (II) Leeds teaches providing an effective as well as security enhanced

mechanism to prevent broadcast traffic storm in the networks by using a email filter associated with an authenticator (Leeds: see for example, Column 1 Line 10 – 16, Column 2 Line 26 – 51).

As per claim 5 and 26, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass further teaches the undesirable pattern of behavior is characterized in that it matches behavior defined by a network administrator as notable or undesirable (Bass: see for example, Column 3 Line 45).

As per claim 6 and 27, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass further teaches the undesirable pattern of behavior is any network pathology characterized as a broadcast storm or an address resolution protocol (ARP) fight (Bass: see for example, Column 3 Line 45 – 65).

As per claim 8 and 29, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass further teaches preventing the dissemination of the undesirable pattern of behavior includes discarding the packets associated with such behavior, isolating any of the computers at which such behavior originates, or isolating any network segments at which such behavior originates (Bass: see for example, Column 3 Line 13 – 65).

As per claim 12 and 33, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass further teaches the network is a shared data network (Bass: see for example, Column 6 Line 50).

As per claim 13 and 32, Bass as modified teaches the claimed invention as described above (see claim 11 and 31 respectively). Bass further teaches the network is a switched Ethernet network and the forwarding device is a switch (Bass: see for example, Column 6 Line 27).

As per claim 14, Bass as modified teaches the claimed invention as described above (see claim 11). Bass further teaches the network is a bridged Ethernet network and the forwarding device is a bridge or a smart bridge (Bass: see for example, Column 10 Line 28).

As per claim 42, Bass as modified teaches a system for limiting the impact of undesirable behavior of computers on a network through which packets of data are interchanged between the computers, comprising:

one or more forwarding devices (Bass: see for example, Column 1 Line 60 – 62); and

one or more packet traffic monitors each including means for monitoring the network for any patterns of behavior, including, if available, information about a pattern

of behavior from any of the computers about another one of the computers; means for determining if the information about the pattern of behavior from any of the computers is trustworthy (Examiner notes (a) the number of multiple destination messages received is interpreted as "information about a pattern of behavior" (Bass: Column 2 Line 48), (b) the network device is interpreted as being used for "monitoring the network" (Bass: Column 2 Line 45 – 58), and (c) the information of monitored multiple destination messages from the said network device about another computers that broadcasts the message to multiple destination computers (Bass: Column 2 Line 45 – 58) is interpreted as "information about a pattern of behavior from any of the computers about another one of the computers" to meet the claim language, where Examiner notes the network device receives the multiple destination messages and categorize the information into one of the broadcast message class and then further validate whether the broadcast message class count exceeds a predefined threshold (Bass: Column 2 Line 45 – 58).

Bass dos not disclose means for determining if the information about the pattern of behavior from any of the computers is trustworthy.

Leeds teaches means for determining if the information about the pattern of behavior from any of the computers is trustworthy (Leeds: Column 7 Line 12 – 13: the receiver would know immediately that the sender is not trustworthy (Leeds: Column 7 Line 12 – 13) and consequently, the information about the pattern of behavior (i.e. email spam) conveyed by the sender is thereby not trustworthy to meet the claim language).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Leeds within the system of Bass

because (I) Bass teaches providing an improved scheme in the prevention or suppression of broadcast traffic storm in computer networks (Bass: Column 2 Line 6 – 8) and (II) Leeds teaches providing an effective as well as security enhanced mechanism to prevent broadcast traffic storm in the networks by using a email filter associated with an authenticator (Leeds: see for example, Column 1 Line 10 – 16, Column 2 Line 26 – 51).

means for determining, upon discovering that one or more of the patterns of behavior is undesirable, a type of the undesirable pattern of behavior (Bass: see for example, Column 3 Line 58 – 62);

means for determining a proper action for mitigating that type of undesirable behavior, the proper action, performed by mitigation means controlling the one or more forwarding devices, including preventing dissemination through the network of packets associated with the undesirable behavior and allowing dissemination of packets not associated with the undesirable behavior (Bass: see for example, Column 3 Line 35 – 57);

As per claim 16 and 35, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Leeds teaches the proper action includes alerting a system administrator about the existence of the undesirable pattern of behavior (Leeds: see for example, Column 7 Line 47).

As per claim 18 and 37, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass does not disclose expressly if available from any one of the computers, the monitored pattern of behavior further includes information about a pattern of behavior by another one of the computers, the method further comprising: determining if the information about the pattern of behavior is trustworthy.

Leeds teaches if available from any one of the computers, the monitored pattern of behavior further includes information about a pattern of behavior by another one of the computers, the method further comprising: determining if the information about the pattern of behavior is trustworthy (Leeds: see for example, Column 7 Line 12 – 13).

See the same rationale of combination as addressed above in rejecting claim 42.

As per claim 19 and 38, Bass as modified teaches the claimed invention as described above (see claim 18 and 37 respectively). Bass does not disclose expressly filters and network configuration parameters are used in determining the trustworthiness.

Leeds teaches filters and network configuration parameters are used in determining the trustworthiness (Leeds: see for example, Column 7 Line 5 – 13).

See the same rationale of combination as addressed above in rejecting claim 42.

As per claim 45, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches the packet traffic monitor is a

separate device connected to the network and through the network to the one or more forwarding devices (Bass: see for example, Column 10 Line 29 and Column 4 Line 54).

As per claim 46, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches one or more of the computers have a dedicated built-in packet traffic monitor (Bass: see for example, Column 10 Line 20 –30).

As per claim 47, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches one or more of the forwarding devices have a dedicated built-in packet traffic monitor (Bass: see for example, Column 10 Line 20 –30).

As per claim 48, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches the network is a switched Ethernet network and forwarding devices are switches (Bass: see for example, Column 6 Line 27).

As per claim 49, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches the one or more forwarding devices include any combination of zero or more switches and routers (Bass: see for example, Column 10 Line 20 – 30).

As per claim 50, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches the network is a bridged network and the forwarding devices are bridges or smart bridges (Bass: see for example, Column 10 Line 28).

As per claim 52, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further teaches the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a high-speed network segment (Bass: see for example, Column 6 Line 51).

As per claim 54, Bass in view of Leeds teaches the claimed invention as described above (see claim 42). Bass further the one or more packet traffic monitors is implemented as a software module (Bass: see for example, Column 10 Line 20 – 30 and Column 4 Line 55 – 57).

5. Claims 2, 9 – 11, 20, 23, 30 – 31 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), and in view of Regan (Patent Number: 6578086).

As per claim 2 and 23, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass as modified does not disclose expressly a discovery, including that of a network topology, facilitates the network monitoring and type of undesirable behavior determination.

Regan teaches a discovery, including that of a network topology, facilitates the network monitoring and type of undesirable behavior determination (Regan: see for example, Column 4 Line 58 – 60, Column 6 Line 40 – 45 and Column 2 Line 11 – 13).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Regan within the system of Bass as modified because (a) Bass as modified teaches identifying the network undesirable behavior such as broadcast storms and (b) Regan teaches providing a mechanism for dynamically managing the topology of a data network to improve the network performance as well as eliminating loops that could lead to broadcast storms essentially crippling network performance (Regan: see for example, Column 2 Line 55 – 63, Column 2 Line 10 – 13 and Column 1 Line 60 – 66).

As per claim 9, Bass as modified teaches the claimed invention as described above (see claim 1). Bass teaches wherein the undesirable pattern of behavior is a broadcast storm; and learning historical packet traffic statistics for any segment of the network (Bass: see for example, Column 1 Line 39 – 44).

Bass as modified does not disclose expressly wherein the monitoring includes recovering a topology of the network using information obtained through a network management protocol interface.

Regan teaches wherein the monitoring includes recovering a topology of the network using information obtained through a network management protocol interface (Regan: see for example, Column 4 Line 58 – 60, Column 6 Line 40 – 45 and Column 2 Line 11 – 13).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Regan within the system of Bass as modified because Regan teaches providing a mechanism for dynamically managing the topology of a data network to improve the network performance (Regan: see for example, Column 2 Line 55 – 63 and Column 1 Line 60 – 66).

As per claim 10, Bass as modified teaches the claimed invention as described above (see claim 9). Bass does not disclose expressly the network management protocol is the simple network management protocol (SNMP). However, Official Notice is taken that the use of SNMP is one of the most widely used methods in the field for network management protocol.

As per claim 11 and 31, Bass as modified teaches the claimed invention as described above (see claim 1 and 23 respectively). Bass does not disclose expressly the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring

includes learning a topology of the network from a forwarding database or table of a forwarding device in the network.

Regan teaches the undesirable pattern of behavior is a broadcast storm, and wherein the monitoring includes learning a topology of the network from a forwarding database or table of a forwarding device in the network (Regan: see for example, Column 3 Line 1 – 10).

See the same rationale of combination as addressed above in rejecting claim 2.

As per claim 20 and 39, Bass as modified teaches the claimed invention as described above (see claim 2 and 23 respectively). Regan further teaches understanding the network topology facilitates disablement of ports in forwarding devices that connect to offending computers (Regan: see for example, Column 6 Line 15 – 25).

As per claim 30, claim 30 does not further teach over claim 9 and 10. Therefore, see same rationale addressed above in rejecting claim 9 and 10

6. Claims 3 – 4 and 24 – 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), and in view of Rodeheffer (Patent Number: 5260945).

As per claim 3 and 24, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass as modified does not disclose expressly the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time.

Rodeheffer teaches the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is lengthened gradually as long as the undesirable behavior continues or intermittently reappears, the time period being gradually shortened if the undesirable behavior stops for a predetermined time (Rodeheffer: see for example, Column 1 Line 42 – 48, Column 2 Line 9 – 45, Column 3 Line 21 – 26 and Column 7 Line 1 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rodeheffer within the system of Bass as modified because (a) Bass as modified teaches identifying the network undesirable behavior that may cause network failures and (b) Rodeheffer teaches providing for an optimized recovery time period of network failures that can minimize the disruption time by considering the information records of failure recovery history (Rodeheffer: see for example, Column 1 Line 13 – 16 and Column 2 Line 34 – 45).

As per claim 4 and 25, as modified teaches the claimed invention as described above (see claim 3, 24 respectively). Rodeheffer further teaches the time period

corresponds to a skepticism level that depends on a history of the undesirable pattern of behavior, a skepticism level zero (0) denoting a good history (Rodeheffer: see for example, Column 3 Line 20 – 26 and Column 5 Line 62 – 67).

7. Claims 7, 15, 17, 28, 34 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), and in view of Arndt (Patent Number: 6826611).

As per claim 7 and 28, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass does not disclose expressly the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

Arndt teaches the undesirable pattern of behavior includes any one or more of a stolen Internet protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many packets directed to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets (Arndt: see for example, Column 1 Line 20 – 25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Arndt within the system of Bass as modified because (a) Bass teaches identifying the network undesirable behavior and (b)

Arndt teaches mitigating the undesirable behavior of traffic pattern in the network by preventing a typical network fault (or one of most common network faults) caused by conflicting and overlapping network traffic associated with mis-configured IP addresses (Arndt: see for example, Column 1 Line 15 – 25).

As per claim 15 and 34, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass as modified does not disclose expressly the undesirable pattern of behavior is too many ARP requests and wherein the monitoring includes verifying stability and lack of conflicts in an IP or MAC address mapping.

Arndt teaches the undesirable pattern of behavior is too many ARP requests and wherein the monitoring includes verifying stability and lack of conflicts in an IP or MAC address mapping (Arndt: see for example, Column 2 Line 5 – 20).

Same rationale of combination addressed herein as above in rejecting claim 7.

As per claim 17 and 36, Bass as modified teaches the claimed invention as described above (see claim 1 and 22 respectively). Bass as modified does not disclose expressly the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address.

Arndt teaches the undesirable pattern of behavior is a simultaneous use of a network address, and wherein the proper action includes disabling any address associated to the network address that contradicts an address list in a network server or disabling any associated address that is not included in a list of addresses that are allowed to map to the network address (Arndt: see for example, Column 3 Line 63 – 65).

Same rationale of combination addressed herein as above in rejecting claim 7.

8. Claims 21 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), in view of Rodeheffer (Patent Number: 5260945), and in view of Singh (Patent Number: 6453430).

As per claim 21 and 40, Bass as modified teaches the claimed invention as described above (see claim 3 and 22). Bass as modified does not disclose expressly the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

Singh teaches the recovery time can be associated with an exponential recovery time interval (Singh: see for example, Column 4 Line 40 – 47).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Singh within the system of Bass as modified because Singh teaches providing significant advancements in fault management for recovery / restart sequence in a real-time or mission critical environments such as data communication networking devices or applications (Singh: see for example, Column 2 Line 32 – 39).

Accordingly, Bass as modified teaches the time period becomes longer in a random exponential backoff before an attempt is made to allow resumption of the packets from any offending computer that originated the undesirable pattern of behavior, the time period becoming longer if the undesirable pattern of behavior reoccurs during a current backoff time, the time period becoming shorter if the undesirable pattern of behavior disappears and does not reoccur in the current backoff time.

9. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), and in view of Regan (Patent Number: 6578086).

As per claim 43, Bass as modified teaches the claimed invention as described above (see claim 42). Bass as modified does not disclose expressly means for

discovery, including that of the network topology, facilitates network monitoring and type of undesirable behavior determination.

Regan teaches means for discovery, including that of the network topology, facilitates network monitoring and type of undesirable behavior determination (Regan: see for example, Column 4 Line 58 – 60, Column 6 Line 40 – 45 and Column 2 Line 11 – 13).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Regan within the system of Bass as modified because Regan teaches providing a mechanism for dynamically managing the topology of a data network to improve the network performance (Regan: see for example, Column 2 Line 55 – 63 and Column 1 Line 60 – 66).

10. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), in view of Singh (Patent Number: 6453430), and in view of Rodeheffer (Patent Number: 5260945).

As per claim 44, Bass as modified teaches the claimed invention as described above (see claim 42). Bass in view of Leeds does not disclose expressly the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is exponentially exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

Singh teaches the recovery time can be associated with an exponential recovery time interval (Singh: see for example, Column 4 Line 40 – 47).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Singh within the system of Bass as modified because (a) Bass as modified teaches identifying the network undesirable behavior such as broadcast storm and (b) Singh teaches providing significant advancements in fault management for recovery / restart sequence in a real-time or mission critical environments such as data communication networking devices or applications (Singh: see for example, Column 2 Line 32 – 39).

Bass as modified does not disclose expressly the recovery time is a time period that is exponentially exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

Rodeheffer teaches a recovery time period exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being shortened if the undesirable behavior stops for a predetermined time (Rodeheffer: see for example, Column 1 Line 42 – 48, Column 2 Line 9 – 45, Column 3 Line 21 – 26 and Column 7 Line 1 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rodeheffer within the system of as modified because (a) Bass in view of Leeds and Singh teaches identifying the network undesirable behavior such as broadcast storm and providing significant advancements

for recovery / restart sequence for data communication networking devices or applications (b) Rodeheffer teaches providing for an optimized recovery time period of network failures that can minimize the disruption time by considering the information records of failure recovery history (Rodeheffer: see for example, Column 1 Line 13 – 16 and Column 2 Line 34 – 45).

Accordingly, Bass as modified teaches the dissemination through the network of packets associated with the undesirable behavior is prevented for a time period that is exponentially exceeding as long as the undesirable behavior continues or intermittently reappears, the time period being exponentially shortened if the undesirable behavior stops for a predetermined time.

11. Claims 51, 55 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), and in view of Johnson (Patent Number: 5640504).

As per claim 51, Bass as modified teaches the claimed invention as described above (see claim 42). Bass as modified does not disclose expressly the one or more packet traffic monitors are placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including one or more locations characterized as being next to an originator of the that behavior, at or next to each

computer, at or next to each forwarding device or at the segment where the packets are to be monitored.

Johnson teaches the one or more packet traffic monitors are placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including one or more locations characterized as being next to an originator of the that behavior, at or next to each computer, at or next to each forwarding device or at the segment where the packets are to be monitored (Johnson: see for example, Column 25 Line 10 – 17 and Column 3 Line 39 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Johnson within the system of Bass as modified because Johnson teaches an effective distributed monitoring and control within a flexible network hierarchy (Johnson: see for example, Column 1 Line 5 – 9).

As per claim 55 and 56, Bass as modified teaches the claimed invention as described above (see claim 42). Bass as modified does not disclose expressly the software module is a part of an operating system.

Johnson teaches the software module is a part of an operating system (Johnson: see for example, Column 25 Line 10 – 17 and Column 3 Line 39 – 42).

See the same rationale of combination as addressed above in rejecting claim 51.

12. Claims 53, 57 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Leeds (Patent Number: 6393465), and in view of Lewis (Patent Number: 6285748).

As per claim 53, Bass as modified teaches the claimed invention as described above (see claim 42). Bass as modified does not disclose expressly the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a place next to or at a network server.

Lewis teaches the one or more packet traffic monitors is placed in a strategic location of the network that is intended to maximize the packet traffic monitor's effectiveness in monitoring and mitigating the patterns of undesirable behavior, the strategic locations including a place next to or at a network server (Lewis: see for example, Column 2 Line 28 – 34 and Figure 3).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Lewis within the system of Bass as modified because Lewis teaches a network traffic monitor and control technique so that the network performance can be optimized (Lewis: see for example, Column 2 Line 27 – 34).

As per claim 57, Bass as modified teaches the claimed invention as described above (see claim 42). Bass as modified does not disclose expressly the one or more packet traffic monitors co-operate with one another in the discovery of the patterns of behavior.

Lewis teaches the one or more packet traffic monitors co-operate with one another in the discovery of the patterns of behavior (Lewis: see for example, Column 6 Line 35 – 48 and Column 8 Line 1 – 20).

See the same rationale of combination as addressed above in rejecting claim 53.

As per claim 58, Bass as modified teaches the claimed invention as described above (see claim 42). Bass as modified does not disclose expressly the one or more packet traffic monitors are configured to sample points on the network randomly or selectively rather than sampling the entire network.

Lewis teaches the one or more packet traffic monitors are configured to sample points on the network randomly or selectively rather than sampling the entire network (Lewis: see for example, Figure 3).

See the same rationale of combination as addressed above in rejecting claim 53.

13. Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Arndt (Patent Number: 6826611).

As per claim 59, Bass teaches a method comprising:

determining a type of the undesirable pattern (Bass: see for example, Column 3 Line 58 – 62); and

determining an action to mitigate the undesirable pattern based on the type of undesirable behavior, the action comprising preventing dissemination over the network of packets associated with the undesirable pattern (Bass: see for example, Column 3 Line 35 – 57).

Bass does not teach monitoring a network for an undesirable pattern comprising at least one of a stolen Internet Protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many probe packets directed to a firewall, and too many address resolution protocol (ARP) packets.

Arndt teaches monitoring a network for an undesirable pattern comprising at least one of a stolen Internet Protocol (IP) address, a stolen media access control (MAC) address, a malformed packet, too many probe packets directed to a firewall, and too many address resolution protocol (ARP) packets (Arndt: see for example, Column 1 Line 20 – 25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Arndt within the system of Bass because (a) Bass teaches identifying the network undesirable behavior and (b) Arndt teaches mitigating the undesirable behavior of traffic pattern in the network by preventing a typical network fault (or one of most common network faults) caused by conflicting and overlapping network traffic associated with mis-configured IP addresses (Arndt: see for example, Column 1 Line 15 – 25).

14. Claim 60 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Arndt (Patent Number: 6826611), and in view of Rodeheffer (Patent Number: 5260945).

As per claim 60, Bass as modified does not disclose expressly preventing the dissemination is performed for .a period of time, the method further comprising:

lengthening the period of time as long as the undesirable behavior continues or intermittently reappears; and shortening the period of time in response to the undesirable behavior stopping for at least a predetermined time (Rodeheffer: see for example, Column 1 Line 42 – 48, Column 2 Line 9 – 45, Column 3 Line 21 – 26 and Column 7 Line 1 – 42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rodeheffer within the system of Bass as modified because (a) Bass as modified teaches identifying the network undesirable behavior that may cause network failures and (b) Rodeheffer teaches providing for an optimized recovery time period of network failures that can minimize the disruption time by considering the information records of failure recovery history (Rodeheffer: see for example, Column 1 Line 13 – 16 and Column 2 Line 34 – 45).

15. Claims 61 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bass (Patent Number: 6185185), in view of Regan (Patent Number: 6578086).

As per claim 61, Bass teaches a system comprising:

a network interface to a network; and a packet traffic monitor to:

monitor the network for an undesirable behavior (Bass: see for example, Column 3 Line 37 – 38);

determine a type of the undesirable behavior (Bass: see for example, Column 3 Line 58 – 62);

Bass does not teach discover a topology of the network; and cause prevention of dissemination over the network of packets associated with the undesirable behavior based on the type of the undesirable behavior and topology of the network.

Regan teaches discover a topology of the network (Regan: Column 6 Line 40 – 45); and

cause prevention of dissemination over the network of packets associated with the undesirable behavior based on the type of the undesirable behavior and topology of the network (Regan: Column 2 Line 10 – 13).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Regan within the system of Bass as modified because (a) Bass as modified teaches identifying the network undesirable behavior such as broadcast storms and (b) Regan teaches providing a mechanism for dynamically managing the topology of a data network to improve the network performance as well as eliminating loops that could lead to broadcast storms essentially

crippling network performance (Regan: see for example, Column 2 Line 55 – 63, Column 2 Line 10 – 13 and Column 1 Line 60 – 66).

As per claim 62, Bass as modified teaches the packet traffic monitor discovers the topology of the network by discovering that the network is one of a router-based network, a bridge-based network, and a switch-based network (Regan: Column 4 Line 57 – 59 and Column 6 Line 40 – 45).

As per claim 63, Bass as modified teaches the prevention of dissemination comprises at least one of changing a routing table, changing a forwarding table, turning off a port of a forwarding device, filtering on an Internet Protocol (IP) address, and filtering on a media access control (MAC) address (Regan: Column 6 Line 13 – 18).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

Longbit Chai
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100